George Haines, Esq.
Nevada Bar No. 9411
Gerardo Avalos, Esq.
Nevada Bar No. 15171
FREEDOM LAW FIRM
8985 S. Eastern Ave., Suite 350
Las Vegas, NV 89123
Tele. 702.880.5554
E-fax: 702.967.6666
Email: info@freedomlegalteam.com

Michael Kind, Esq.
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Phone: (702 337-2322
FAX: (702) 329-5881
Email: mk@kindlaw.com
Attorneys for Plaintiffs Marina Cardenas and Susie Frazier-Telles, and on behalf of all others similarly situated

EIGHTH JUDICIAL DISTRICT COURT

CLARK COUNTY, NEVADA

Marina Cardenas and Susie Frazier-Telles, individually and on behalf of all others similarly situated,

Plaintiffs,

-vs.-

Super Care, Inc., dba SuperCare Health,

Defendant.

CASE NO.

Dept. No.:

CLASS ACTION

Complaint for Damages Based on: (1) Negligence; (2) Invasion of Privacy; (3) Breach of Contract; (4) Breach of Implied Contract; And (5) Violation of NRS 598

Jury Trial Demanded

Introduction

1. Defendant SuperCare Health, Inc., (hereinafter "Defendant" and/or SuperCare) failed to safeguard the confidential personal identifying information of Plaintiffs Marina Cardenas and Susie Frazier-Telles ("Plaintiffs") and thousands of individuals (hereinafter referred to as "Class Members" or collectively as the "Class"). This class action is brought on behalf of patients whose personally identifiable information ("PII" or "Private Information") was stolen by cybercriminals in a cyber-attack that accessed sensitive patient information through SuperCare's services.

2. From July 23, 2021 to July 27, 2021, a group of cybercriminals had access to certain files on Defendant's computer network and servers containing personal information belonging to the Class Members.

3. Plaintiffs and Class Members were not notified of the data breach until March 25, 2022, more than eight months after their information was first accessed.

4. The cybercriminals accessed insufficiently protected information belonging to Plaintiffs and the Class Members. Upon information and belief, as a result of Defendant's failure to properly secure Plaintiffs' and the Class Members' personal information, the cybercriminals obtained extensive personal information including names, addresses, email addresses, dates of birth, Social Security numbers, health insurance billing information, and treating physician information, collectively known as personally identifiable information ("PII" or "Private Information").

5. As a result of Defendant's actions and/or inaction, Plaintiffs and the Class Members were harmed and forced to take remedial steps to protect themselves from future loss. Indeed, Plaintiffs and all of the Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their financial accounts.

6. Defendant's wrongful actions and/or inaction constitute common law negligence, invasion of privacy by the public disclosure of private facts, breach of contract, and breach of implied contract.

7. Plaintiffs, on behalf of themselves and the Class seeks (i) actual damages, economic damages, emotional distress damages, statutory damages and/or nominal damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

Jurisdiction and Venue

8. This Court has jurisdiction to hear this case.

9. Plaintiffs are residents of Clark County, Nevada. Defendant is a corporation organized and existing by virtue of the laws of the State of Nevada and registered with the Nevada Secretary of State. Defendant conducts business in the State of Nevada, County of Clark.

10. The transactions and occurrences that give rise to Plaintiffs' claims against Defendant occurred in Clark County, Nevada.

11. Therefore, the Eighth Judicial District Court, Clark County, Nevada has personal jurisdiction over both Plaintiffs and Defendant and subject matter jurisdiction pursuant to Article 6, Section 6 of the Nevada Constitution and NRS 4.370.

Parties

12. Plaintiffs are natural persons residing in Clark County, Nevada.

13. Defendant is a respiratory treatment company, which operates nationally, including in Nevada. SuperCare offers a number of respiratory treatment products, including PAP supply testing, iSleep testing, recurrent prescriptions refills CPAP supplies, Prescriptions Oxygen Concentrators and other respiratory-focused services.

Factual Allegations

14. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

15. According to the Federal Trade Commission ("FTC"):

> Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing

> damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

16. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

17. Healthcare Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices

18. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

19. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed by Defendant.

20. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

    a. Know what personal information you have in your files and on your computers;

    b. Keep only what you need for your business;

    c. Protect the information that you keep;

d. Properly dispose of what you no longer need;

e. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

21. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

22. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

23. The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

24. HIPPA requires that covered entities like SuperCare protect against reasonably anticipated threat to the security of Private Information. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PII. Safeguards must include physical, technical, and administrative components.

25. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

26. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

27. Upon information and belief, Defendant has policies and procedures in place regarding the safeguarding of confidential information it is entrusted with and Defendant failed to comply with those policies. Defendant also negligently failed to comply with industry standards or

even implement rudimentary security practices, resulting in Plaintiffs' and the Class' confidential information being substantially less safe than had this information been entrusted with other similar companies.

28. In or around March 2022, Plaintiffs and thousands of Class Members received letters from Defendant notifying them that it learned of suspicious activity that allowed one or more cybercriminals to access its systems through a ransomware attack. The March 2022 Notice disclosed that a ransomware attack enabled a threat actor to access SuperCare systems.

29. The criminals were able to access Plaintiffs' personal information because Defendant failed to take reasonable measures to protect the Personally Identifiable Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

30. SuperCare's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many patients were affected by the Data Breach.

31. As a result of Defendant's failure to properly secure Plaintiffs' and the Class Members' personal identifying information, Plaintiffs' and the Class Members' privacy has been invaded.

32. Moreover, all of this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiffs' and the Class Members' unencrypted, non-redacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, policy numbers, and more.

33. Given all of the information obtained, the criminals would also be able to create numerous fake accounts and sell sensitive health information, as part of their identity theft operation.

34. As a direct and proximate result of Defendant's wrongful disclosure, criminals now have Plaintiffs' and the Class Members' personal identifying information. Additionally, the disclosure makes Plaintiffs and Class Members much more likely to respond to requests from Defendant or law enforcement agencies for more personal information, such as bank account numbers, login information or even Social Security numbers. Because criminals know this and are capable of posing as Defendant or law enforcement agencies, consumers like Plaintiffs and their fellow Class Members are more likely to unknowingly give away their sensitive personal information to other criminals.

35. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum.

36. Defendant's wrongful actions and inaction here directly and proximately caused the public disclosure of Plaintiffs' and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendant's wrongful actions and/or inaction, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

37. Plaintiffs and Class Members are now required to monitor their accounts and to respond to identity theft. Plaintiffs and Class Members now face a very high risk of identity theft.

38. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

39. Despite disregarding its obligations to protect the sensitive information that Plaintiffs and Class Members entrusted it with, Defendant has not offered Plaintiffs and Class Members any monetary compensation or even assistance with identity protection services.

40. SuperCare was at all times fully aware of its obligation to protect the Private Information of its patients because of its position as a trusted healthcare provider. SuperCare was also aware of the significant repercussions that would result from its failure to do so.

Class Action Allegations

41. Pursuant to Rule 23 of the Nevada Rules of Civil Procedure, Plaintiffs bring this class action on behalf of themselves and the following Class of similarly situated individuals:

> All persons whose sensitive personal information, including, but not limited to, names, home addresses, dates of birth, driver's licenses, and social security numbers was obtained by an unauthorized individual or individuals from Defendant during the July 2021 data breach.

42. The Class specifically excludes Defendant and its officers, directors, agents and/or officers, the Court, and Court personnel.

43. The putative Class is comprised of over 3,000 persons, making joinder impracticable. The joinder of the Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the Court. The Class can be identified through Defendant's records or Defendant's agents' records.

44. The rights of each Class Member were violated in an identical manner as a result of Defendant's willful, reckless and/or negligent actions and/or inaction.

45. The questions of law and fact common to all Class Members, and which predominate over any questions affecting only individual Class Members, are as follows:

a. Whether Defendant negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' personal identifying information;

b. Whether Defendant was negligent in storing and failing to adequately safeguard Plaintiffs' and Class Members' personal identifying information;

c. Whether Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their personal identifying information;

d. Whether Defendant breached its duties to exercise reasonable care in failing to protect and secure Plaintiffs' and Class Members' personal identifying information;

e. Whether by disclosing Plaintiffs' and Class Members' personal identifying information without authorization, Defendant invaded Plaintiffs' and Class Members' privacy;

f. Whether Defendant created an implied contract with Plaintiffs and Class Members to keep their personal identifying information confidential; and

g. Whether Plaintiffs and Class Members sustained damages as a result of Defendant's failure to secure and protect their personal identifying information.

46. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' attorneys are highly experienced in the prosecution of consumer class action, complex litigation and privacy breach cases.

47. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Defendant's wrongful disclosure of their personal identifying information and from Defendant's failure to properly secure and protect the same.

48. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been irreparably harmed as a result of Defendant's wrongful actions and/or inaction.

49. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's failure to secure and protect Plaintiffs' and Class Members' personal identifying information.

50. Class certification, therefore, is appropriate pursuant to Rule 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

51. Class certification also is appropriate pursuant to Rule 23 of the Nevada Rules of Civil Procedure because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

52. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendant will retain the benefits of their wrongdoing despite its serious violations of the law.

First Cause of Action
Negligence

53. Plaintiffs repeat, re-allege, and incorporate by reference all above paragraphs.

54. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

55. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

56. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' personal identifying information would result in an unauthorized third party gaining access to such information for no lawful purpose, and that such third parties would use Plaintiffs' and Class Members' personal identifying information for malevolent and unlawful purposes, including the commission of direct theft and identity theft.

57. Defendant knew, or should have known, of the risks inherent in collection and storing Private Information and the importance of adequate security. Defendant knew of should have known about numerous well-publicized data breaches within the medical industry.

58. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket

expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they suffered loss and are entitled to compensation.

59. Defendant's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) negligence at common law.

Second Cause of Action
Invasion of Privacy by Public
Disclosure of Private Facts and Intrusion Upon Seclusion

60. Plaintiffs repeat, re-allege, and incorporate by reference all above paragraphs.

61. Plaintiffs' and Class Members' personal identifying information is and always has been private information.

62. Dissemination of Plaintiffs' and Class Members' private information is not of a legitimate public concern; publication to third parties of their personal identifying information would be, is and will continue to be, offensive to Plaintiffs, Class Members, and other reasonable people.

63. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they are entitled to compensation.

64. Defendant's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their personal identifying information).

Third Cause of Action
Breach of Contract

65. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

66. Plaintiffs and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class Members agreed to provide their Private Information to Defendant, and Defendant agreed to provide medical services and, impliedly, if not explicitly, agreed to protect Plaintiffs' and Class Members' Private Information.

67. These contracts include HIPAA privacy notices and explanation of benefits documents.

68. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class Members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. Neither Plaintiffs nor any Class member would have entered into these contracts with Defendant without the understanding that Plaintiffs' and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

69. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

70. The protection of Plaintiffs' and Class Members' Private Information were material aspects of Plaintiffs' and Class Members' contracts with Defendant.

71. Defendant's promises and representations described above relating to HIPAA and industry practices, and Defendant's purported concern about its clients' privacy rights became terms of the contracts between Defendant and its clients, including Plaintiffs and other Class Members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

72. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by SuperCare and/or otherwise understood that SuperCare would protect its patients' Private Information if that information were provided to SuperCare.

73. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

74. As a result of Defendant's breach of these terms, Plaintiffs and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the lost difference in the value between the secure

health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, the requirement to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports. Additionally, and Plaintiffs and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

75. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and fees and costs of litigation.

Fourth Cause of Action
Breach of Implied Contract

76. Plaintiffs repeat, re-allege, and incorporate by reference all above paragraphs.

77. "Where the terms of a contract are literally complied with but one party to the contract deliberately contravenes the intention and spirit of the contract, that party can incur liability for breach of the implied covenant of good faith and fair dealing." *Hilton Hotels Corp. v. Butch Lewis Prods., Inc.*, 107 Nev. 226, 232 (1991).

78. Among other things, Plaintiffs and Class Members were required to disclose their personal identifying information to Defendant for the provision of healthcare services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

79. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

80. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

81. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

82. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide medical services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and Class Members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

83. The implied contracts for the provision of fertility testing services, contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter and Defendant's Notice of Privacy Practices.

84. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

85. Plaintiffs and Class Members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

86. Defendant materially breached its contractual obligation to protect the private information Defendant gathered when the information was accessed and exfiltrated during the Data Breach.

87. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class Members' private information as set forth above.

88. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

89. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive full benefit of the bargain they entered into, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

90. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

91. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

Fifth Cause of Action
Violation of Nevada Deceptive Trade Practices Act
Nev. Rev. Stat. §598, et Seq.

92. Plaintiffs repeat, re-allege, and incorporate by reference all above paragraphs.

93. This cause of action is brought pursuant to the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§598 *et seq.*, (the "Nevada Act").

94. Defendant is a healthcare provider that sells goods and services to the general public. Defendant's activities are governed by the State Consumer Protection Acts.

95. On information and belief, affected individuals include persons over the age of 60 and persons with disabilities.

96. In all requisite matters alleged herein, Defendant acted in the course of their business or occupation within the meaning of NRS §§598.0903 to 598.0999.

97. In all requisite matters alleged herein, Defendant acted willfully in violation of NRS §598.

98. Defendant violated NRS §598 by engaging in the unfair and deceptive practices as described herein which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers.

99. Reasonable customers would be misled by Defendant's misrepresentations and omissions concerning the security of their personally identifying information. Defendant's unfair and deceptive practices are thus likely to, and have, misled the Class Members acting reasonably in the circumstances, in violation of NRS §598.

100. Defendant specifically engaged in the following activity, all of which violate NRS §598:

a. Defendant failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' personal identifying information;

b. Defendant acted unlawfully in improperly storing and failing to adequately safeguard Plaintiffs' and Class Members' personal identifying information;

c. Defendant failed to exercise reasonable care in protecting and securing their personal identifying information;

d. Defendant failed to properly and timely notify Plaintiffs and the Class about the severity of the breach, including failure to provide an adequate description of the breach and the risks associated with the breach.

101. In all requisite matters alleged herein, Defendant acted knowingly within the meaning of NRS §598.

102. In all requisite matters alleged herein, Defendant acted willfully in violation of NRS §598.

103. Defendant violated, among other sub provisions of NRS §598, NRS §598.0923(3) when it violated HIPPA, as discussed above.

104. Plaintiffs have been aggrieved by Defendant's unfair and deceptive practices including because they have lost control of their personally identifying information, and they have to expend out of pocket money and efforts to mitigate the harm caused by Defendant.

105. Pursuant to NRS §598, Plaintiffs and the Class Members seek a declaratory judgment and court order enjoining the above-described wrongful acts and practices of Defendant. Additionally, Plaintiffs and the Class Members make claims for damages, and fees and costs of litigation.

Prayer for Relief

106. Wherefore, Plaintiffs, individually and on behalf of the other members of the Class proposed in this complaint, respectfully request that the Court enter judgement in favor of Plaintiffs and the Class against Defendant, as follows:

- Certifying this action as a class action, with a class as defined above;
- For equitable relief enjoining Defendant from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- Awarding compensatory damages to redress the harm caused to Plaintiffs and Class Members in the form of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of- pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm. Plaintiffs and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiffs' and Class Members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court.
- Ordering injunctive relief including, without limitation, (i) adequate credit monitoring, (ii) adequate identity theft insurance, (iii) instituting security protocols in compliance with the appropriate standards and (iv) requiring Defendant to submit to periodic compliance audits by a third party regarding the security of personal identifying information in its possession, custody and control.
- Awarding Plaintiffs and the Class Members interest, costs and attorneys' fees; and
- Awarding Plaintiffs and the Class such other and further relief as this Court deems just and proper.

Trial by Jury

107. Pursuant to the seventh amendment to the Constitution of the United States of America and the Constitution of the State of Nevada, Plaintiffs is entitled to, and demands, a trial by jury.

DATED this 7th day of April 2022.

FREEDOM LAW FIRM, LLC

/s/ Gerardo Avalos
George Haines, Esq.
Gerardo Avalos, Esq.
8985 South Eastern Ave., Suite 350
Las Vegas, NV 89123
Attorneys for Plaintiffs and on behalf of all others similarly situated

KIND LAW

/s/ Michael Kind
Michael Kind, Esq.,
NV Bar No. 13903
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
Attorneys for Plaintiffs and on behalf of all others similarly situated